(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 44 20 967 A1**

(51) Int. Cl.[6]: H 04 L 9/28

(21) Aktenzeichen: P 44 20 967.3
(22) Anmeldetag: 16. 6. 94
(43) Offenlegungstag: 21. 12. 95

DE 44 20 967 A1

(71) Anmelder:

ESD Vermögensverwaltungsgesellschaft mbH, 80333 München, DE

(74) Vertreter:

Haußingen, P., Ing. Faching. f. Schutzrechtswesen, Pat.-Anw., 06526 Sangerhausen

(72) Erfinder:

Antrag auf Nichtnennung

(56) Entgegenhaltungen:

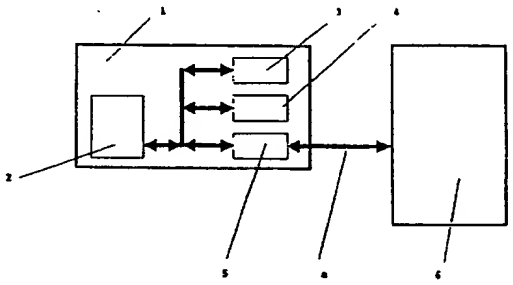
DE	31 24 150 C2
DE	34 32 721 A1
GB	22 14 677 A
US	53 13 521
US	52 37 611
US	49 91 208
US	49 07 273
US	48 87 296
US	41 82 933
EP	5 06 435 A2
JP	5-1 22 217 A2

PRESTTUN, K.: Sicherungsfunktionen in Nachrichtennetzen. In: Elektrisches Nachrichtenwesen, Bd.60, Nr. 1, 1986, S.63-70;

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Entschlüsselungseinrichtung von digitalen Informationen und Verfahren zur Durchführung der Ver- und Entschlüsselung derselben

(57) Die Erfindung betrifft eine Entschlüsselungseinrichtung von digitalen Informationen und Durchführung der Ver- und Entschlüsselung derselben.
Die Aufgabe ist es, eine Vorrichtung und ein Verfahren zu entwickeln, nach denen die Schlüssel mit öfter wechselnden Verschlüsselungsalgorithmen verschlüsselt werden sollen, wobei bestimmte Schlüssel für bestimmte Personen verfügbar sein müssen und die Verteilung der Schlüssel und der Schutz vor Entschlüsselung gegeben ist.
Erfindungsgemäß wird die Aufgabe dadurch gelöst, daß die Entschlüsselungseinrichtung aus einem integrierten Schaltkreis (1), dem ein Zentralprozessor CPU (2), ein interner nichtauslesbarer flüchtiger Speicher mit wahlfreiem Zugriff RAM (3) als Arbeitsspeicher und ein interner nichtauslesbarer nichtflüchtiger Speicher mit wahlfreiem Zugriff ROM (4) und ein Interface (5) zugeordnet sind, indem sich jede Entschlüsselungseinrichtung von jeder weiteren unterscheidet durch den Inhalt des internen nichtflüchtigen Speichers mit wahlfreiem Zugriff ROM (4) und teilweise in einem integrierten Schaltkreis integriert ist und daß das Interface (5) zwischen dem Zentralprozessor CPU (2) und dem Personalcomputer (6) angeordnet ist und mit dem Zentralprozessor CPU (2) mit dem Datenpfad (a) verbunden sind.



DE 44 20 967 A1

Beschreibung

Die Erfindung betrifft eine Entschlüsselungseinrichtung von digitalen Informationen und das Verfahren zur Durchführung der Ver- und Entschlüsselung derselben, indem die Entschlüsselungseinrichtung Berechtigten den Zugriff gewährt und Unberechtigte vom Zugriff ausschließt.

Digitale Informationen werden in immer größerem Maßstab über unsichere Verteilungskanäle versandt. Diese Informationen sollen aber sicherzustellen, daß nur die berechtigte Person den Schlüssel erhält und die Information entschlüsseln kann. Die Schlüsselübergabe muß so gestaltet werden, daß es nur berechtigten Personen möglich ist, die Schlüssel zu nutzen und die Weitergabe unmöglich ist.

In der Patentschrift US 84/01856 wird ein Ver-/Entschlüsselungsapparat (EDU) beschrieben. Diese Erfindung verfolgt das Ziel, den sicheren Schlüsselaustausch über ungesicherte Datenleitungen (z. B. Telefonanleitungen) zu ermöglichen. Jede EDU enthält einen Zentralprozessor (CPU), Speicher mit wahlfreiem Zugriff (ROM), in welchem Schlüsselaustauschschlüssel (KEK) gespeichert sind und einen "data-encryption standard" (DES) Koprozessor; alles in einem Keramikmodul eingebettet, um die Untersuchung der Befehlsabarbeitung unmöglich zu machen. Weiterhin enthält jede EDU einen Spezialschaltkreis, welcher es der CPU ermöglicht, verschlüsselte Befehle abzuarbeiten. Bei Aufnahme einer Verbindung zwischen zwei EDU's wählt jede EDU einen Teilschlüssel. Dieser Teilschlüssel wird verschlüsselt an die Gegenstelle übertragen und geprüft. Danach werden beide Teilschlüssel zum sogenannten Sessionkey zusammengesetzt. Mit diesem Sessionkey wird dann die Information verschlüsselt und übertragen.

Ein Nachteil dieser Erfindung ist, daß eine Verbindung in beide Richtungen nötig ist, um den Schlüssel auszutauschen. Dies ist bei dieser Methode auch nötig, da beide EDU's jeweils einen Teil des Schlüssels erzeugen, der dann zur jeweils anderen EDU übertragen und zum vollständigen Schlüssel zusammengesetzt wird. Weiterhin ist es auf diese Weise nicht möglich, Informationen an Empfängergruppen mit der gleichen Verschlüsselung zu versenden, da für jede Verbindung zweier EDU's ein anderer Schlüssel generiert wird.

Die Patentschrift EP 0266748 beschreibt einen Koprozessor mit Entschlüsselungseigenschaften und nichtauslesbaren Schlüsseltafeln. Diese Schlüsseltafeln werden mit einem Übergabemodul in den Koprozessor übertragen. Bei der Übertragung der Schlüsseltafel für ein bestimmtes Programm in den Koprozessor wird das Übergabemodul entwertet. Dadurch wird ein mehrfaches Übertragen der Schlüsseltafel in mehrere Koprozessoren verhindert. Damit ist es dann möglich, Programme, zu denen die Schlüsseltafel in den Koprozessor übertragen wurden, zu entschlüsseln.

Der Nachteil dieser Erfindung, ist jedoch, daß die Übergabe eines Transfertokens in einem speziellen Speicher (Hardware-Übergabemodul) zu erfolgen hat, der dann bei der Benutzung entwertet wird. Dies bringt natürlich Handlingprobleme mit sich. Dieses Modul muß an den Endkunden weitergeleitet werden. Es ist dann auch keine nochmalige Entschlüsselung der Information möglich, da das Übergabemodul entwertet wurde. Weiterhin ist keine Schlüsselübergabe über elektronische Medien möglich.

Um die oben genannten Nachteile des Standes der Technik zur Verteilung von Informationen zu beheben, ist es Aufgabe der Erfindung ein Verfahren zu schaffen, mit dem Informationen bedienerfreundlich an mehrere Empfänger verteilt werden können, sowie einen geringen verwaltungstechnischen Aufwand zur Informationsverschlüsselung hat.

Es besteht also die Notwendigkeit, ein Verfahren zu finden, mit der es möglich ist, Schlüssel sicher zu verteilen und die Übertragung dieser gegen Erkunden zu schützen.

Weiterhin ist es notwendig, daß es selbst dem Besitzer eines Entschlüsselungsgerätes nicht möglich ist, einen Schlüssel weiterzugeben.

Um diese Forderungen zu erfüllen, ist es möglich, die Schlüssel in irgendeiner Weise zu verschlüsseln.

Die modernen Möglichkeiten zum Brechen eines Verschlüsselungsalgorithmus beruhen auf dem Vorhandensein von sogenannten Plaintexten (unverschlüsselte Information) und der dazugehörigen Ciphertexte (verschlüsselte Information). Um Blocksysteme, wie z. B. den DEA zu brechen, muß die Menge diese Texte sehr groß sein. Dies ist notwendig um solche Methoden wie die differentielle Cryptoanalyse von Biham und Shamir durchzuführen. Diese Methode ist der beste zur Zeit bestehende Angriff auf Bockverschlüsselsysteme wie den DEA (beschrieben in Eli Biham und Adi Shamir "Differential Cryptoanalysis of DES-like Cryptosystems" in Journal of Cryptology vol. 4 pp 3—72, 1991).

Ein Erkunden des Verschlüsselungsverfahrens des Schlüssels soll aber weitgehend erschwert werden.

Es ist also nötig, die Menge der Dritten zur Verfügung stehenden Plain-/Ciphertexte möglichst gering zu halten, was besonders bei der Schlüsselübergabe nötig ist.

Dies erreicht man dadurch, daß die Schlüssel mit öfter wechselnden Verschlüsselungsalgorithmen verschlüsselt werden. Dritte, welche die Schlüssel entschlüsseln wollen, müssen dann jedesmal einen neuen "Knackalgorithmus" entwickeln, wenn das Verschlüsselungsverfahren gewechselt wird.

Weiterhin ist es damit möglich, bestimmte Schlüssel nur für bestimmte Personen und auch Personenkreise verfügbar zu machen, indem diesen das Entschlüsselungsverfahren für Schlüssel zugänglich gemacht wird.

Es ist ebenfalls nötig, einen Spezialprozessor als Teil dieses Verfahrens zu schaffen, der die Verteilung der Schlüssel ermöglicht, sowie sowie den Schutz von Entschlüsselungsverfahren der Schlüssel vor Weitergabe preiswert und sicher realisiert.

Ebenfalls notwendig ist es, daß es auch den rechtmäßigen Empfängern eines Entschlüsselungverfahrens für Schlüssel nicht möglich ist, diese weiterzugeben.

Erfindungsgemäß wird diese Aufgabe durch die im Patentanspruch 1 und Patentanspruch 2 angegebenen Merkmale gelöst. Bevorzugte Weiterbildungen ergeben sich aus den Unteransprüchen.

Die Erfindung wird nachstehend anhand der Fig. 1, die die Entschlüsselungseinrichtung von Entschlüsselungsalgorithmen für Schlüssel zeigt und dem Verfahren zur Durchführung der Ver- und Entschlüsselung von digitalen Informationen, dargestellt.

Die in Fig. 1 dargestellte Entschlüsselungseinrichtung von Entschlüsselungsalgorithmen von Schlüsseln wird zur Verdeutlichung anhand eines Einsatzes in mehreren Personalcomputern gezeigt, wobei digitale Informationen an ausgewählte Besitzer von Entschlüsselungseinrichtungen gesandt werden.

Dabei besteht die dargestellte Entschlüsselungseinrichtung aus einem integrierten Schaltkreis 1, dem ein Zentralprozessor CPU 2, ein interner nichtauslesbarer

flüchtiger Speicher mit wahlfreiem Zugriff RAM 3 als Arbeitsspeicher und ein interner nichtauslesbarer nichtflüchtiger Speicher mit wahlfreiem Zugriff ROM 4 (in welchem zwei interne nichtauslesbare Entschlüsselungsalgorithmen (EI und EA) gespeichert sind) und ein Interface 5 zugeordnet sind, welches zwischen dem Zentralprozessor CPU 2 und dem Personalcomputer 6 angeordnet ist und mit dem Personalcomputer 6 mit dem Datenpfad a verbunden ist, und teilweise in einen integrierten Schaltkreis integriert ist.

Die Übertragung eines Entschlüsselungsalgorithmus für Schlüssel an eine Entschlüsselungseinrichtung geschieht wie folgt:

Der Verteiler wählt einen Verschlüsselungsalgorithmus (EEU). Dieser sei zum Verschlüsseln der später übertragenen Schlüssel gedacht. Dieser Verschlüsselungsalgorithmus muß natürlich geheim gehalten werden und muß weiterhin sicher genug sein um Sicherheit bei der Verschlüsselung von Schlüsseln zu bieten. Dafür würden sich z. B. verschiedene Abarten des DES (z. B. mit verschiedenen S-Boxen) oder andere Verschlüsselungsverfahren eignen.

Nun wird der zum Verschlüsselungsalgorithmus (EEU) passende Entschlüsselungsalgorithmus (EE) zum unleserlichen Algorithmus (EEV) verschlüsselt.

Nun kann jeder Benutzer einer Entschlüsselungseinrichtung, der einen Schlüssel erhalten will, sich bei der Verteilerstelle melden. Dies kann z. B. verbal (auch über Telefon), schriftlich oder elektronisch erfolgen. Anhand der öffentlichen Seriennummer der Entschlüsselungseinrichtung muß er sich identifizieren. Da diese Seriennummer nur einmal vergeben wird, ist es der Entschlüsselungseinrichtung möglich, die Entschlüsselungseinrichtung und deren Besitzer eindeutig zu identifizieren. Die Verteilungsstelle kann nun darüber entscheiden, ob der Empfänger berechtigt ist, den Entschlüsselungsalgorithmus zu empfangen. Das kann auch von einer Bezahlung abhängen.

Wenn dies geklärt ist, wird der verschlüsselte Entschlüsselungsalgorithmus (EEV) zum Benutzer der Entschlüsselungseinrichtung übertragen und dort im der Entschlüsselungseinrichtung zum Algorithmus (EE) entschlüsselt.

Nun ist es möglich Schlüssel, die mit dem Verschlüsselungsalgorithmus (EEU) verschlüsselt wurden, zu entschlüsseln.

Dies soll nun an einem Ausführungsbeispiel dargestellt werden.

Es soll eine Menge von digitalen Informationen an ausgewählte Kunden versandt werden. Dabei soll allen die gesamte Information übertragen werden, aber nicht alle Kunden sollen den Zugriff auf alle Informationen haben. Eine preiswerte Realisierung dafür stellt z. B. die Verteilung dieser Informationen per CD-ROM dar. Diese Datenträger sind in großen Stückzahlen preiswert zu produzieren und können sehr große Datenmengen speichern. Es liegt also nahe, alle Informationen verschlüsselt auf einer CD-ROM unterzubringen an alle Kunden zu senden, und dann nur noch die Berechtigung die Informationen zu nutzen an die Kunden zu verteilen. Diese Berechtigung soll mit dieser Erfindung folgendermaßen übertragen werden.

Es seien nun die CD's an alle Kunden verteilt. Weiterhin sei Kunde A im Besitz der Entschlüsselungseinrichtung mit der Seriennummer SN = 1.

Nun soll der Kunde A die Information B erhalten. Diese Information liegt auf der CD-ROM mit dem zum gewöhnlichen internen Entschlüsselungsalgorithmus (EA) passenden Verschlüsselungsalgorithmus (EAU) unter Nutzung des Schlüssels (K) nach

$$NV := EAU(NE, K)$$

verschlüsselt.

Jetzt muß der Kunde A noch den Schlüssel erhalten.

Dazu wird beim Verteiler der Informationen die Übergabe des Schlüssels an die Entschlüsselungseinrichtung vorbereitet. Es wählt der Verteiler der Informationen einen Verschlüsselungsalgorithmus (EEU), welcher dann zur Verschlüsselung des später zu übertragenden Schlüssels genutzt werden soll. Dieser Verschlüsselungsalgorithmus wird nie offen, sondern nur in verschlüsselter Form übertragen.

Der Hersteller der Entschlüsselungseinrichtung/die Verteilerstelle der Informationen verfügt in einer Datenbank über die internen Entschlüsselungsalgorithmen (EI) und auch die zugehörigen Verschlüsselungsalgorithmen (EIU) aller an Kunden aus gegebenen Entschlüsselungseinrichtungen.

Es sei EI1, der interne Entschlüsselungsalgorithmus (EI) der Entschlüsselungseinrichtung (mit der internen Seriennummer SN = 1) beim Kunden A. Weiterhin sei EI1U, der ebenfalls nur dem Hersteller der Entschlüsselungseinrichtung bekannte Verschlüsselungsalgorithmus passend zu EI1.

Nun wird der, der Entschlüsselungseinrichtung zu übertragende Schlüssel (K) verschlüsselt. Dies erfolgt in der Art, daß dieser mit dem zu übertragenden Entschlüsselungsalgorithmus (EE) passenden Verschlüsselungsalgorithmus (EEU) zum unleserlichen Schlüssel (S) nach folgender Formel verschlüsselt wird:

$$S := EEU(K).$$

Dieser verschlüsselte Schlüssel (S) wird der Entschlüsselungseinrichtung übertragen.

Um diesen Schlüssel zu entschlüsseln benötigt die Entschlüsselungseinrichtung beim Kunden A natürlich ebenfalls den Entschlüsselungsalgorithmus EE. Da dieser aber geheimgehalten werden muß, wird er in verschlüsselter Form übertragen.

Dies erfolgt in der Art, daß der Entschlüsselungsalgorithmus (EE) mit dem zum internen Entschlüsselungsalgorithmus (EI) der Entschlüsselungseinrichtung passenden Verschlüsselungsalgorithmus (EIU) zum unleserlichen Algorithmus (EEV) nach folgender Formel verschlüsselt wird:

$$EEV := EIIU(EE).$$

Dieser verschlüsselte Algorithmus (EEV) wird der Entschlüsselungseinrichtung beim Kunden A übertragen.

Dies kann z. B. verbal (auch über Telefon), schriftlich oder elektronisch erfolgen.

Der übermittelte verschlüsselte Algorithmus und der verschlüsselte Schlüssel sind relativ kurz. Damit ist ein Knacken des internen Entschlüsselungsalgorithmus der Entschlüsselungseinrichtung (EI) schwer möglich. Wie oben gezeigt, müssen für ein Brechen der Verschlüsselung viele Plain- und Ciphertexte vorhanden sein, um erfolgversprechende Knackalgorithmen verwenden zu können. Dies ist aber in diesem Fall wegen der geringen Menge der übermittelten Information schwer möglich.

Nun wird beim Empfänger das Entschlüsselungsgerät funktionstüchtig gemacht.

Der Ablauf beim Einschalten der Versorgungsspannung oder nach einer Unterbrechung der Abarbeitung ist folgender:
Der Zentralprozessor CPU 2 führt mit dem internen nichtauslesbaren nicht flüchtigen Speicher mit wahlfreiem Zugriff ROM 4 und dem internen nichtauslesbaren flüchtigen Speicher mit wahlfreiem Zugriff RAM 3 einen Selbsttest durch. Dies könnte z. B. durch eine Prüfsummenbildung geschehen.

Der Entschlüsselungsalgorithmus in verschlüsselter Form (EEV) wird nun beim Kunden in vom Benutzer der Entschlüsselungseinrichtung in den Personalcomputer 6 eingegeben oder in anderer Form eingelesen.

Nun erfolgt das Einlesen des verschlüsselten Entschlüsselungsalgorithmus (EEV) in die Entschlüsselungseinrichtung über das Interface 5.

Als nächstes wird mit Hilfe des im internen nichtauslesbaren nichtflüchtigen Speicher mit wahlfreiem Zugriff ROM 4 gespeicherten Entschlüsselungsalgorithmus (EI) der verschlüsselt vorliegende Entschlüsselungsalgorithmus (EEV) mit dem internen Entschlüsselungsverfahren (EI) entschlüsselt. Dies geschieht in der Weise, daß der Zentralprozessor CPU 2 die im internen nichtauslesbaren nicht flüchtigen Speicher mit wahlfreiem Zugriff ROM 4 gespeicherten Anweisungen des Entschlüsselungsalgorithmus (EI) ausführt und den verschlüsselten Entschlüsselungsalgorithmus (EEV) folgendermaßen entschlüsselt:

$$EE := EII(EEV).$$

Bei diesem Verfahren entsteht wieder, da der interne Entschlüsselungsalgorithmus (EI1) mit dem Verschlüsselungsalgorithmus (EIU1) zusammenpaßt mit dem der Entschlüsselungsalgorithmus (EE) verschlüsselt wurde, der ursprüngliche Entschlüsselungsalgorithmus (EE).

Dieser wird im internen nichtauslesbaren flüchtigen Speicher mit wahlfreiem Zugriff RAM 3 abgespeichert und ist somit nicht von außen erkundbar. Damit ist es nicht möglich, den Entschlüsselungsalgorithmus weiterzugeben, da er in verschlüsselter Form wertlos ist und in unverschlüsselter Form nicht vorliegt.

Nun ist die Entschlüsselungseinrichtung einsatzbereit und es ist nun die Möglichkeit gegeben, den Schlüssel (K) zu berechnen.

Die Entschlüsselung eines Schlüssels, der an den Kunden in verschlüsselter Form übertragen wurde erfolgt folgendermaßen:
Die CPU lädt über das Interface 5 den Schlüssel (S).

Nun wird mit Hilfe der nichtauslesbaren Schlüsselberechnungsfunktion EE in der Entschlüsselungseinrichtung der Schlüssel berechnet nach:

$$K := EE(S).$$

Dieser Schlüssel (K) ist nie außerhalb der Entschlüsselungseinrichtung zu finden und auch nicht erkundbar. Damit ist es niemandem möglich diesen weiterzugeben.

Nun wird die Information von der CD-ROM vom Interface 6 geladen.

Als nächstes wird sie mit dem vom Zentralprozessor CPU 2 mit dem gewöhnlichen Entschlüsselungsalgorithmus der Entschlüsselungseinrichtung (EA) unter Nutzung des Schlüssels K entschlüsselt.

$$NE := EA(NV, K).$$

Danach wird die entschlüsselte Information (NE) von dem Zentralprozessor CPU 2 über das Interface ausgegeben und steht dem Kunden zur Verfügung.

Damit gelingt es, den Zugriff auf die verschlüsselten Informationen flexibel zu gestalten. Weiterhin besteht die Möglichkeit, bestimmten Gruppen von Empfängern oder einzelnen Empfängern Teile der Information einer CD-ROM zugänglich zu machen ohne, daß es diesen möglich ist, die Schlüssel weiterzugeben. Damit gelingt es, Schlüssel mit verschiedenen Verschlüsselungsalgorithmen zu verschlüsseln und mit verschiedenen Entschlüsselungseinrichtungen zu entschlüsseln, ohne daß der Entschlüsselungsalgorithmus bekannt gemacht werden muß oder vorher schon in der Entschlüsselungseinrichtung vorliegt.

Weiterhin ist der übertragene Entschlüsselungsalgorithmus für Schlüssel weder weitergebbar noch erkundbar, da er individuell für jedes Entschlüsselungsgerät verschlüsselt übertragen wird, dort nichtauslesbar gespeichert und nur zum internen Gebrauch des Entschlüsselungsgerätes mit der entsprechenden Seriennummer verfügbar ist. Es wird damit die Möglichkeit geschaffen, auch Entschlüsselungseinrichtungen vom Informationsempfang auszuschließen.

Bezugszeichenliste

1 integrierter Schaltkreis
2 Zentralprozessor CPU
3 interner nichtauslesbarer flüchtiger Speicher mit wahlfreiem Zugriff RAM
4 interner nichtauslesbarer nichtflüchtiger Speicher mit wahlfreiem Zugriff ROM
5 Interface
6 Personalcomputer
a Datenpfad

Verwendete Abkürzungen

CPU = Zentralprozessor
DEA = data encryption standard
EA Entschlüsselungsalgorithmus intern zur Entschlüsselung von Informationen
EAU = Verschlüsselungsalgorithmus beim Verteiler der Informationen zur Verschlüsselung der Informationen passend zu EA
EI = Entschlüsselungsalgorithmus intern zur Entschlüsselung von übertragenen Entschlüsselungsalgorithmen
EI1 = Entschlüsselungsalgorithmus intern für die Entschlüsselungseinrichtung mit der Seriennummer SN = 1
EIU = zum internen Entschlüsselungsalgorithmus (EI) passender Verschlüsselungsalgorithmus
EI1U = zum internen Entschlüsselungsalgorithmus (EI1) passender Verschlüsselungsalgorithmus für die Entschlüsselungseinrichtung mit der Seriennummer SN = 1
EE = Entschlüsselungsalgorithmus zur Entschlüsselung von verschlüsselten Schlüsseln
EEV = verschlüsselter Entschlüsselungsalgorithmus
EEU = Verschlüsselungsalgorithmus passend zu EE
NE = nichtverschlüsselte oder entschlüsselte Information
NV = verschlüsselte Information
Schlüssel K = Schlüssel zur Entschlüsselung von Nachrichten
Schlüssel S = mit dem Verschlüsselungsalgorithmus (EEU) verschlüsselter Schlüssel zur Entschlüsselung von Nachrichten
(:=) = ergibt sich aus.

Patentansprüche

1. Entschlüsselungseinrichtung von digitalen Informationen, **dadurch gekennzeichnet**, daß vom Verteiler des Entschlüsselungsalgorithmus dieser mit einem Verschlüsselungsalgorithmus (EIU) verschlüsselt wird, welcher dem Entschlüsselungsalgorithmus (EI) entspricht, der in der jeweiligen empfangenden Entschlüsselungseinheit intern vorhanden ist, und daß der Entschlüsselungsalgorithmus (EI) der Öffentlichkeit nicht zugänglich und auch nicht erkundbar ist, daß der Nutzer der Entschlüsselungseinrichtung den verschlüsselten Entschlüsselungsalgorithmus in die Entschlüsselungseinrichtung eingibt und dieser innerhalb der Entschlüsselungseinrichtung entschlüsselt wird, daß die Entschlüsselungseinrichtung aus einem integrierten Schaltkreis (1), dem ein Zentralprozessor CPU (2), ein interner nichtauslesbarer flüchtiger Speicher mit wahlfreiem Zugriff RAM (3) als Arbeitsspeicher und ein interner nichtauslesbarer nichtflüchtiger Speicher mit wahlfreiem Zugriff ROM (4) und ein Interface (5) zugeordnet sind, indem sich jede Entschlüsselungseinrichtung von jeder weiteren unterscheidet durch den Inhalt des internen nichtflüchtigen Speichers mit wahlfreiem Zugriff ROM (4) und teilweise in einem integrierten Schaltkreis integriert ist und daß das Interface (5) zwischen dem Zentralprozessor CPU (2) und dem Personalcomputer (6) angeordnet ist und mit dem Zentralprozessor CPU (2) mit dem Datenpfad (a) verbunden sind.

2. Entschlüsselungseinrichtung von digitalen Informationen und Verfahren zur Durchführung der Ver- und Entschlüsselung derselben dadurch gekennzeichnet, daß im

1. Schritt

vom Verteiler des Entschlüsselungsalgorithmus dieser mit einem, nur dem Hersteller der Entschlüsselungseinrichtung bekannten Verschlüsselungsalgorithmus (EIU), welcher dem Entschlüsselungsalgorithmus (EI) in der Entschlüsselungseinheit entspricht, wie folgt verschlüsselt wird:

$$EEV := EIU(EE)$$

und dieser verschlüsselte Algorithmus (EEV) der Entschlüsselungseinrichtung übertragen wird, wonach im

2. Schritt

die Entschlüsselungseinrichtung, mit dem Zentralprozessor CPU (2) mit dem internen nichtauslesbaren nichtflüchtigen Speicher mit wahlfreiem Zugriff ROM (4) einen Selbsttest durchführt, und das Einlesen des verschlüsselten Entschlüsselungsalgorithmus (EEV) in das Entschlüsselungsgerät über das Interface (5) erfolgt und nun mit Hilfe des im internen nichtauslesbaren nichtflüchtigen Speicher mit wahlfreiem Zugriff ROM (4) gespeicherten Entschlüsselungsalgorithmus (EI) der verschlüsselt vorliegende Entschlüsselungsalgorithmus (EEV) mit dem internen Entschlüsselungsverfahren (EI) nach

$$EE := EI(EEV)$$

entschlüsselt wird, wobei bei diesem Verfahren wieder der ursprüngliche Entschlüsselungsalgorithmus (EE) entsteht, welcher im

3. Schritt

im internen nichtauslesbaren flüchtigen Speicher mit wahlfreiem Zugriff RAM (3) abgespeichert, und somit nicht von außen erkundbar ist, womit die Entschlüsselungseinrichtung mit dem Entschlüsselungsalgorithmus (EE) einsatzbereit ist und die Entschlüsselung eines Schlüssels (S) im

4. Schritt

folgendermaßen erfolgt, daß die CPU über das Interface (5) den Schlüssel S, lädt und der Schlüssel von dem Zentralprozessor CPU (2) mit dem Entschlüsselungsalgorithmus (EE) entschlüsselt wird, nach

$$K := EE(S),$$

und der Schlüssel damit für die Entschlüsselung der Information zur Verfügung steht und im

5. Schritt

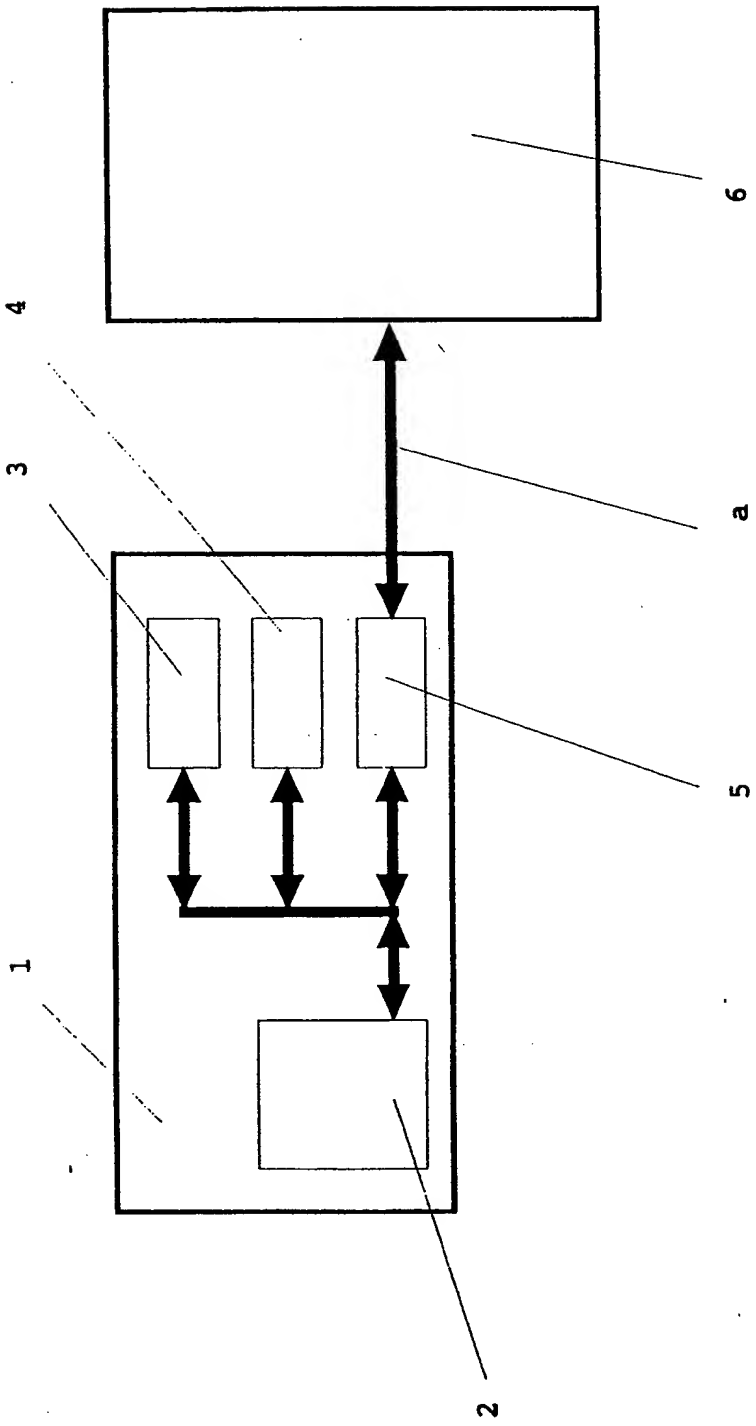
die digitale Information und mit dem internen Entschlüsselungsalgorithmus (EA) unter Nutzung des Schlüssels (K) welcher nicht außerhalb des integrierten Schaltkreises erscheint, von dem Zentralprozessor CPU (2) nach

$$NE := EA(NV,K),$$

entschlüsselt und von dem Zentralprozessor CPU (2) über das Interface (5) ausgegeben wird und dem Empfänger zur Verfügung steht.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 44 20 967 A1
Int. Cl.[6]: H 04 L 9/28
Offenlegungstag: 21. Dezember 1995



Figur 1